APPLICATIONS OF SIGNAL PROCESSING IN DIGITAL COMMUNICATIONS

Final Technical Report
by
Michele Elia

April 1991

United State Army
EUROPEAN RESEARCH OFFICE OF THE U.S.ARMY
London England

R & D No. 5228-CC-01

Contract Number DAJA45-86-C-0044

Dipartimento di Elettronica - Politecnico di Torino
Corso Duca degli Abruzzi 24 - I-10129 Torino, Italy

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER 7	2. GOVT ACCESSION NO.	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) Applications of Signal Processing in Digital Communications		5. TYPE OF REPORT & PERIOD COVERED FINAL REPORT 1987-90 6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s) MICHELE ELIA		8. CONTRACT OR GRANT NUMBER(s) DAJA45-86-C-0044
9. PERFORMING ORGANIZATION NAME AND ADDRESS Dipartimento di Elettronica Politecnico di Torino Corso D. Abruzzi 24 - I10129 Torino (I)		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS
11. CONTROLLING OFFICE NAME AND ADDRESS U.S.Army Research, Development & Standardization GRoup - UK		12. REPORT DATE April 1991 13. NUMBER OF PAGES 36
14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office)		15. SECURITY CLASS. (of this report) Unclassified 15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Digital Communications, Group Codes, Computational Complexity
Concatenated codes

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

In this report we summerize our general considerations on the design of signal sets and coding schemes. The aim is to provide a set of rules that are behind an efficient use of the transmission resources. In particular we discuss the basis signal design, point constellations, combined coding/modulation, and concatenation of codes, which appear to be the present day qualified artifices that exchange complexity for bandwidth, transmission rate and power.

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

ABSTRACT

In this report we summarize our general considerations on the design of signal sets and coding schemes. The aim is to provide a set of rules that are behind an efficient use of the transmission resources. In particular we discuss the basis signal design, point constellations, combined coding/modulation, and concatenation of codes, which appear to be the present day qualified artifices that exchange complexity for bandwidth, transmission rate and power.

TABLE OF CONTENTS

1. Introduction
2. Channels
3. Base waveforms
4. Point constellations
5. Modulation schemes
6. Coding schemes
7. Complexity analysis
8. Conclusions
9. List of Research Publications 1987-1990 (Appendices A-G)
10. References

Enclosure: Appendices A-G

1 - Introduction

The research activity during the three-years period covered by this final report was essentially directed to study the section of a transmission chain that is allocated between the channel encoder and the channel decoder enclosed. That is the part of a communication system that properly carries the information from the sender side to the receiver end. In particular we have considered the following topics:

1) The problem of the basis waveforms and their generation.

2) Signal sets and group point constellations.

3) Modulation: combined codes and signals.

4) Code concatenation: combination criteria that yield optimal performance after complete decoding.

5) Complexity of arithmetical operations in finite fields.

The idea behind was to describe and present a set of rules and conditions representing the guidelines for the design of signals and codes, the objects that appear to be the principal components of any communication link.
This subject of course is the central matter of communication theory so the whole set of available results cannot be certainly summarized in a short report, neither we have such a presumption. But our limited scope is to point out some aspects that not always have received the attention that they deserve. We hope that our little effort will contribute to a better comprehension of the fundamental phenomena that regulate the transmission of the information.
Specifically in this report after having recalled the general model of any communication chain, we successively describe the peculiar functions of the main building components with reference to the special topics considered in our previous technical reports. In particular section 3 is dedicated to the study of basis waveforms and section 4 consider the point constellations. In section 5 a short description of general combination schemes for coding and modulation is reported and in section 6 a strategy as well as an algorithm for the correction of both errors and erasures by means of Reed Solomon codes are described. Finally in section 7 considerations on the complexity of the arithmetical operations in finite fields are reported.

At last this conclusive report tries to give a hopefully convincing motivation of our apparently dispersed interest on scattered topics shown by the list of the research publications. In our opinion we have fractionally reviewed the wide range of tools that we consider to be the indispensable reference notions for every designer of transmission systems.

1.1 - The Model

After Shannon's fundamental ideas about the description of every communication system which were masterly exposed in his seminal paper *A Mathematical theory of Communication*, it is definitively accepted that the model of a transmission chain is composed by the concatenation of functional blocks that describe either information transformations or the behavior of the physical supports used to transfer the information.
The basis skeleton consists of the chain **source-channel-user**, however the more detailed scheme represented in fig. 1 must be considered for any particular investigation. In fig. 1 we distinguish the following relevant blocks:

SOURCE - The source produces the information to be transferred. It may be described abstractly as a *scheme* characterized by a finite alphabet $\mathcal{A} = \{a_i\}_{i=1}^{M}$ with an associated distribution probability $p\{a_i\}, i = 1 \ldots M$. However for study purposes of the transmission scheme only, it is more conveniently viewed as a mechanism that emits, every T seconds, one of M equiprobable symbols from the alphabet $\mathcal{A}$.

Channel encoder - The encoder usually performs two tasks:

- It maps the source symbols into symbols of an alphabet (usually elements of a finite field $GF(q)$) suitable for encoding operations.
- It operates the encoding by adding parity check symbols to the information symbols according to the error correcting code used.

Modulator - It maps channel encoder symbols into a convenient set of signals to be sent on the channel. The signals may be either baseband or translated into a suitable band, in every case they may be described by means of a finite set of basis waveforms that define a finite dimensional signal space. The transmitted digital signal may be written as

$$m(t) = \sum_{-\infty}^{\infty} S_{\xi_k}(t - kT) \quad ,$$

where $S_{\xi_k}(t)$ are signals of finite duration T selected from a finite set $\{S_i(t)\}_{i=1}^{N}$ according to a rule governed by a random variable ξ_k that assumes N possible integer values.

CHANNEL - It is the physical support on which the waveforms are sent. It is characterized by deterministic physical parameters that allow us to specify the transformation affecting the waveforms during the propagation and by stochastic parameters that allow us to describe the non-deterministic transformations that corrupt the conveyed signals. These unpredictable modifications are called noise and ultimately motivate all processing both at the transmitting and receiving sides.

Demodulator - It performs the dual operation of the modulator, that is it converts the received signals into channel code symbols. However its function is more complex because of the presence of noise: it must practically solve the theoretical impossible problem of inverting a map that is not one to one. Therefore the demodulator assignment is to guess, according to proper strategies, the signal that has been sent given a received signal corrupted by noise, this inevitably introduces the errors.

Channel decoder - The decoder has the same objective as the demodulator: it also has to invert a function that was deliberately not one to one because of the introduction of the parity check symbols that expand the true dimension of the information space. In other words it attempts to correct the noise introduced errors.

USER - It is the final destination at which the information is directed, usually the information is received encoded into the source alphabet and then it is converted in a meaningful form for the applications.

In this scenario the principal aim is to recover at the user front end the useful information in the most faithful and economical manner. In mathematical terms, more frequently, this means to keep the symbol error probability as small as possible, with constrained resources, i.e. with limited energy, bandwidth and complexity of the devices. However, apparently in contradiction with the last statement, it must be remarked that not always error probability is the proper measure of quality, other characteristics may be more important, for example voice or musical sound quality in radio broadcasting, imperfect image restoration but nevertheless informative in tomography, etc.

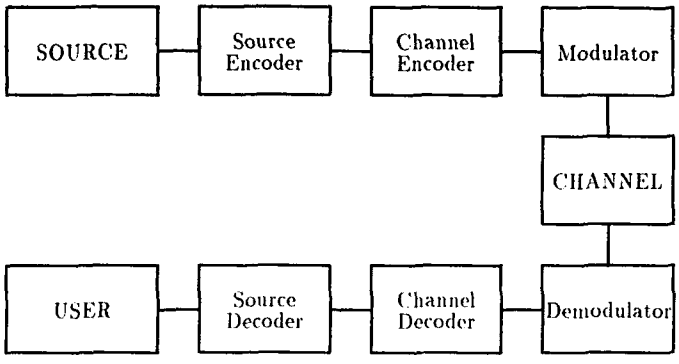

Figure 1: Transmission chain model

2 - Channels

The channels are very complex admixture of devices, structures, physical resources and random components. In general they are a concatenation of the following objects:

- The modulator which generates and sends the signals on the channel.
- The electrical, optical or acoustical means used to convey the waveforms that carry the information properly encoded. This is the channel properly said in our model on which the signals are corrupted by noise, interferences and by the behavior of imperfect devices. The noise is described by the frequency spectrum and the stochastic parameters. The other sources of impairments have descriptions which may be deterministic or stochastic.
- The demodulator usually tries to recover the information signal sent from the distorted received signal.

The signal space is a n-dimensional vector space specified by a set of n basis waveforms of finite duration T:

$$\{\varphi_j(t)\}_{j=1}^{n} \quad .$$

These waveforms are used to construct the signal set according to the rule

$$S_i(t) = \sum_{j=1}^{n} x_{ji}\varphi_j(t) \qquad 1 \leq i \leq M \quad ,$$

where the set of vectors

$$\mathbf{X}_i = (x_{1i}, x_{2i}, \ldots, x_{ni}) \qquad i = 1, \ldots M$$

is called code for the noisy channel (frequently Gaussian channel) and constitutes a point configuration in a n-dimensional real vector space.

The channel properly said may be described as a stochastic mechanism that adds to the signal $m(t)$ unwanted disturbances such as noise $\nu(t)$, interferences $I(t)$ and distortions $D(t)$, so that the received signal will be:

$$r(t) = m(t) + \nu(t) + I(t) + D(t) \quad .$$

Obviously all of these impairments have a convenient mathematical description which may be either exhaustive or incomplete depending on causes that not always are under the user's control.

3 - Base waveforms

The design of base signals has been extensively investigated with different aims in many fields of science, for a good account by one of the majors contributors see [55]. However the subject accidentally remains at a purely speculation level and has not received the deserved attention by the communication engineers. This is possibly due to the consolidated experience in generating sinusoids and typical baseband waveforms, to the existence of firmly established standards and, why not, to the traditional human conservatism. At last it must be said that also a theoretical argument motivates this apparently casual choice, because as it was acutely observed by Slepian, [55], a large number of communication systems can be modeled by linear transformations that admit sinusoidal functions as eigenfunctions.
Good books have been exclusively dedicated to the subject, see for example [36], where the design of base signal has received a convenient attention and a general accurate formulation in mathematical terms. By the way the actual trend in technological environments maintains the supremacy for sine and cosine signals as well as the definitively unavoidable baseband signals.

Inconveniences such as intersymbol and co-channel interferences are controlled by using equalization (i.e. post-processing) and filter shaping. In our opinion this consolidated traditional approach could be integrated by paying more attention to the design of the base signal set, limiting the intrinsic impairments with pre-processing instead of post-processing. In the following we will try to outline this approach with no pretension of completeness.

The slightly different point of view that tries to obtain a base signal set more adapted to the channel is based on the results concerning the problem of the *Maximum transfer of energy with constraints both in*

bandwidth and time.

This problem has been variously considered as research subject during the past. Deep theoretical results appeared in the early sixties in papers by Slepian and others. It will be now formally stated in order to emphasize the relevant mathematical aspects and the lines of possible future studies towards the feasibility of practical applications.
Let us consider the set $\mathcal{S} = \{s_i(t)\}_{i=1}^{n}$ of signals strictly limited in time at the interval [0. T], and having finite energy, i.e.

$$\int_0^T s(t)^2 dt < \infty \quad .$$

Let the signals be sent over a linear channel characterized by the linear transfer function $h(t)$ so that the output signal $y(t)$ is

$$y(t) = \int_{-\infty}^{\infty} h(t-\tau)s(\tau)d\tau \quad .$$

The problem is to find the signal $s(t)$ such that the corresponding output signal $y(t)$ has the maximum energy concentrated in a limited frequency interval $[-W/2,\ W/2]$.
The solution of this problem is proposed in [36], where also useful examples are developed such as the ideal pass-band filter and the first order Butterworth filter. Whereas solutions for the whole class of Butterworth filters has been reported in [29, 30]. It is interesting to recall some of these results in order to illustrate what can be expected and the amount of signal processing required in the design of new and efficient signal sets.
The problem is conveniently formulated as a computation of the norm of an

integral linear operator in a proper Hilbert space. It is well known and it will be briefly reviewed hereafter, that the square of this norm represents the maximum of the energy of signals passed through a filter characterized by the operator. The most studied operator of this kind is certainly the bandlimiting operator with kernel $\frac{\sin t}{t}$ whose eigenfunctions, the prolate spheroidal functions, are connected to basilar theorems on time and bandlimited functions [55].

Let $\|x\|$ denote the euclidean norm of a function x in a given Hilbert space $\mathcal{H}$, let $\mathcal{N}(\mathbf{V})$ denote the norm of a bounded linear operator $\mathbf{V}$ acting in $\mathcal{H}$, therefore $\mathcal{N}(\mathbf{V})$ is defined as a constrained maximum

$$\mathcal{N}(\mathbf{V}) = \max_{\|x\|=1} \|\mathbf{V}x\| \quad .$$

The simplest way to compute this maximum is to look for the maximum of the square $\|\mathbf{V}x\|^2$, therefore $\mathcal{N}(\mathbf{V})$ will result from the solution of the classical problem of constrained maxima for positive quadratic forms. It is well known, [50], that $\mathcal{N}(\mathbf{V})^2$ is given by the greatest eigenvalue σ_{max} of the linear operator $\mathbf{V}\mathbf{V}^*$, i.e.

$$\mathbf{V}\mathbf{V}^* x = \sigma_{max} x \quad ,$$

where $\mathbf{V}^*$ denotes the adjoint operator of $\mathbf{V}$ and $\|\mathbf{V}x\|^2 = \sigma_{max}$.
If $\mathbf{V}$ is an operator with kernel $k(t)$ associated to a linear filter then

$$y(t) = \mathbf{V}x(t) = \int_{-\infty}^{\infty} k(t-s)x(s)ds$$

is the filtered signal. The energy of $y(t)$ is

$$\|y\|^2 = \|\mathbf{V}x\|^2 = \int_R y(t)^2 dt = \int_R \int_R \int_R k(t-s)k(t-u)x(s)x(u)duds dt$$

$$= \int_R \int_R h(u-s)x(s)x(u)duds$$

where

$$h(u-s) = \int_R k(t-s)k(t-u)dt$$

is the kernel of $\mathbf{V}\mathbf{V}^*$.
The square $\mathcal{N}(\mathbf{V})^2$ of the norm of $\mathbf{V}$ is given by the maximum eigenvalue σ_1 of $h(t)$ with associated the eigenfunction $\psi_1(t)$ limited in time, i.e.

$$\int_0^T h(t-u)\psi_1(u)du = \sigma_1 \psi_1(t) \quad . \tag{1}$$

The eigenvalue σ_1 yields the maximum allowance of the energy of any finite duration signal passed through the filter. The associated eigenfunctions may become important subjects because they provide an orthonormal basis $\{\psi_i(t)\}_{i=1}^{n}$ for any finite set of digital signals. To solve equation (1) is usually very difficult, however special classes of operators allow us get closed form solutions by standard techniques. Let us consider operators $\mathbf{Q}$ with symmetric kernel of the form $K(t,s) = h(t-s)$ whose inverse $\mathbf{Q}^{-1}$ is a purely differential linear operator of the form

$$\mathbf{Q}^{-1} = \sum_{i=0}^{k} a_i(s)(\frac{d}{ds})^i \quad .$$

The eigenfunctions of $\mathbf{Q}^{-1}$ are solutions of a linear differential equation, which in many interesting cases can be explicitly solved. Therefore, since commuting operators have the same set of eigenfunctions, we can find the eigenvalues of $\mathbf{Q}$ by using the eigenfunctions of the differential operator $\mathbf{Q}^{-1}$, see [29]. A large class of operators, with practical significance, have kernels $h(t)$ whose Fourier transforms is the reciprocal of an even polynomial, an interesting example is provided by the second order filters, i.e.

$$H(f) = \frac{1}{1 + 2a(f/W)^2 + (1-2a)(f/W)^4} \qquad 0 < a < 1/2 \quad .$$

It is clarifying to outline the main computations that explicitly produce the eigenvalues. As said before the procedure is two steps

i) given $H(f)$ find the general solution of the differential equation associated to $H(f)^{-1}$;

ii) impose this solution to be an eigenfunction of $\mathbf{Q}$ to obtain a condition (usually a transcendental equation), for the eigenvalues and finally compute the eigenfunctions [29].

The eigenfunctions for a second order filter satisfy a differential equation of fourth order

$$\frac{d^4\psi}{ds^4} - \frac{8a\pi^2W^2}{1-2a}\frac{d^2\psi}{ds^2} - (\frac{1}{\sigma} - 1)\frac{(4\pi^2W^2)^2}{(1-2a)}\psi = 0 \qquad (2)$$

whose characteristic equation has roots that can be denoted as

$$2\pi WX,\ -2\pi WX,\ 2\pi jWY,\ -2\pi jWY$$

where

$$X = \sqrt{\frac{a + \sqrt{\Delta}}{1 - 2a}} \quad and \quad Y = \sqrt{\frac{-a + \sqrt{\Delta}}{1 - 2a}}$$

are real numbers connected by the relation

$$X^2 - Y^2 = \frac{2a}{1 - 2a}$$

and $\Delta = a^2 + (1 - 2a)(\frac{1}{\sigma} - 1)$. It follows that the eigenfunctions of $\mathbf{V}$ will have the general form

$$\varphi(t) = c_1\, e^{2\pi WXt} + c_2\, e^{-2\pi WXt} + c_3\, e^{2\pi iWYt} + c_4\, e^{-2\pi iWYt} \qquad (3)$$

where the four constants c_i's are found as a solution of a linear homogeneous system of algebraic equations and σ is root of a transcendental equation obtained by imposing that $\varphi(t)$ is eigenfunction of the integral operator, i.e. by requiring that

$$\int_I h(t - s)\varphi_i(s)ds = \sigma_i\varphi_i(t) \quad .$$

be an identity. Set

$$\sigma = \frac{1}{1 - 2aX^2 + (1 - 2a)X^4} \quad .$$

from the resulting homogeneous system in four unknowns, ($a \neq \sqrt{2} - 1$), we get a transcendental equation that yields X and in turn σ. The equation for X is very complex, here we report only its asymptotic expression for great values of X:

$$tg(2\pi WTX) = \pm\frac{X}{4} + \frac{3}{2X} + O(\frac{1}{X^2}) \quad ,$$

showing that we have an infinity of roots because of the periodicity of the tangent function.

It has been shown that the increase of the dimension of the signal space yields a better use of the channel resources, at the relatively limited increasing in complexity. We can in fact summarize some of the advantages that can be deduced from the completion of the above argument

1. the increase of the product $2WT$ automatically ameliorates both the co-channel and the intersymbol interference because it allows us to use basis waveforms with better concentrations of energy both in time and frequency.

2. the signal pre-processing allows us to reduce the receiver complexity with possibly a better use of the computational power.

3. from the forced greater dimension of the signal space we are constrained to use large signal sets with the unavoidable condition of choosing such sets to approximate the Shannon bounds. [43].

From the above considerations we can conclude that basis signals space of larger dimension should be considered in the future. Moreover it should be hopefully better if such signals will be matched with the channel characteristics. Here we have resorted some tools that should deserve a better attention by the designers of data links.

3.1 - Synchronization aspects

Synchronization has always been one of the most critical issue in any transmission system. The well known problem consists in

> Given a finite duration signal $\varphi(t)$ transmitted on a channel of limited bandwidth, therefore from the received signal $r(t)$ find the proper time allocation t_0 for $\varphi(t - t_0)$, which maximizes the correlation
>
> $$\int_0^T r(t)\varphi(t + t_0)dt \quad .$$

The devices for synchronization acquisition usually are quite complicated and normally represent an expensive part of any receiving device. The use of improper basis signals that are sensitive to synchronization problems may cancel the advantages coming from the believed convenient conditions that were imposed in their construction.
In this context synchronization capabilities may be evaluated by considering a set of cross-correlation relations defined as follows.
Given the set of basis waveforms $\{\psi_i(t)\}_{i=1}^n$ of finite duration T, their cross-correlation functions are defined as

$$\phi_{ij}(\tau) = \int_0^T \psi_i(t)\psi_j(t + \tau)dt \quad .$$

If the functions $\psi_i(t)$ satisfy equation (1) with the companion operator $\mathbf{Q}^{-1}$ time-invariant, then it is immediately seen that $\phi_{ij}(\tau)$ is an eigenfunction associated to the eigenvalue σ_j. It follows that, in general, synchronization is a critical issue for this kind of waveforms and the maximum concentration

of energy is not always the best target to be pursuit. However we can be more optimistic because in certain circumstances we may have positive return. Let us assume that $\mathbf{Q}^{-1}$ is also invariant for time-reverse. Define the cross-correlation functions as follows

$$\Phi_{ij}(\tau) = \int_{-\infty}^{\infty} \psi_1(t)\psi_j(t+\tau)dt \quad .$$

We have

$$\Phi_{ij}(\tau) = \int_{-\infty}^{\infty} \psi_1(t-\tau)\psi_j(t)dt \quad ,$$

showing that $\Phi_{ij}(\tau)$ is an eigenfunction for both σ_i and σ_j and therefore is identically zero, unless $i = j$. In this last instance it results

$$\Phi_{ii}(\tau) = A\psi_i(\tau) \quad ,$$

and therefore the reference time can be recovered from the zero crosses of $\Phi_{ii}(\tau)$.

4 - Point constellations

The Kotelnikov geometrical representation of the signals has assumed a prominent position in all descriptions of signal carrying information. Many Shannon heuristic results have been achieved by purely geometric arguments. The flavor of the geometric view has lead to results otherwise unreachable.

The representation of signals by points in n-dimensional vector spaces $\mathcal{R}_n$ permitted almost naturally to consider symmetry, a feature that seems unavoidable to approach the performance guaranteed by the information-theoretical bounds. Therefore the machinery of group representation and the intuitive results, pictorially appealing, of n-dimensional geometry are used to describe and to produce point configurations that present the more convenient features for generating signal sets.

The geometry of the point constellations as well as associated geometrical object such as Voronoi (or decision) regions have a role in the computation of the signal performance over channels with rotational invariance. This topic has assumed a relevant position in the design of any modulation scheme, far beyond the initial status when the subject was considered just amateurishly or without a real engineering concern. The paper [28] is intended to review the state of the art in this sector. Other surveys appeared before, the most

relevant is [12], and the recent survey [24] is interesting. The analysis of a large but finite number of regular configurations of points in n-dimensional spaces, point constellations that usually are associated a transitive group of symmetry, is a challenging problem.

The consideration of group codes leads to enhance different achievable gains

1. increased space dimension yields two advantages:
   (a) possibility of using more valid basis signals;
   (b) gain coming from the greater minimum distance achievable per dimension;
2. greater is the number of available configurations larger is the number of constraints that can be accomplished.

In [28] is reported a configuration with 16 points in dimension 4 that shows a minimum square distance of 1.17 with a gain, normalized with respect to the space dimension, of 1.65 dB over the 16-QAM in dimension 2. Moreover a second advantage coming from the four dimensional point constellation is that the corresponding signals have constant envelope.

5 - Modulation schemes

The ever increasing interest in combined modulation and coding after the pioneering Ungerboeck's paper is motivated by the high performance obtained at moderate complexity.
Two combination principle have become prominent:

- Trellis Code Modulation (TCM) is a technique that combines convolutional codes and modulation, the demodulation is executed by means of the Viterbi algorithm that uses a metric induced by the signal constellation;
- Block Code Modulation (BCM) is a technique that combines block codes and modulation, the demodulation is performed by using a euclidean metric induced by the signal constellation, that is a euclidean distance is computed between the received signal and any possible transmitted signal.

Therefore in order to devise decoding rules affording manageable complexities both codes and modulations must accomplish strong symmetry conditions. Symmetries of geometrical objects are mathematically described by the action of finite groups of transformations, so henceforth we will assume that both error correcting codes and multidimensional signal sets have nice symmetry groups.

5.1 - A general combining principle

Let us briefly describe a general principle for combining error control codes and modulations. This approach in many circumstances produces signal sets decodable by algorithms of restrained complexity.
Let us consider a set of L channel error correcting codes $\mathcal{C}_i$ respectively with symbols from the alphabet $\mathcal{A}_i$, codeword length n_i, cardinality M_i and minimum Hamming distance d_i, for $i = 1, \ldots, L$. Possibly all codes have a common codeword length N. Suppose that each code is associated to a symmetry group which may be

> either a group of transformations generating the whole set of codewords starting from an initial set,
>
> or the code itself has a group structure with a subset of codewords as generators.

Let us define their *external* product

$$\mathcal{Q} = \bigotimes_i \mathcal{C}_i \quad .$$

as the set of L-dimensional vectors with the first entry coming from any codeword of $\mathcal{C}_1$, the second entry coming from any codeword of $\mathcal{C}_2$ and so on until the L-th entry coming from any codeword of $\mathcal{C}_L$. To avoid border effects, if the codeword lengths are different then we must think of unlimited concatenations of codewords.
Let us consider a group code $[M, n]$ which is a n-dimensional point configuration $\mathcal{P}$ generated by the action, of a representation of a group $\mathcal{G}$, on an initial set of points. Let us consider the coset partition of $\mathcal{G}$ with respect the subgroup $\mathcal{H}_1$ with transversal $\mathcal{T}_1$:

$$\mathcal{G} = \bigcup_{t_1 \in \mathcal{T}_1} t_1 \mathcal{H}_1 \quad ,$$

such that the condition $\mid \mathcal{T}_1 \mid = \mid \mathcal{A}_1 \mid$ is accomplished. Moreover let us assume that a chain of subgroups exists

$$\mathcal{G} \supset \mathcal{H}_1 \supset \mathcal{H}_2 \ldots \supset \mathcal{H}_L \quad ,$$

with each transversals $\mathcal{T}_i$ satisfying the condition $\mid \mathcal{T}_i \mid = \mid \mathcal{A}_i \mid$, $i = 1, \ldots L$. Therefore let us consider the hierarchical partition of $\mathcal{P}$ induced by the above described partition of $\mathcal{G}$.

> A combined modulation and coding scheme is specified by an invertible mapping Φ, from $\mathcal{Q}$ into $\mathcal{P}$, induced by the correspondences
>
> $$\phi_i \quad : \mathcal{A}_i \longrightarrow \mathcal{T}_i \qquad i = 1, \ldots, L \quad .$$

This combining technique is accompanied by a number of theorems that demonstrate how the coding gain can be achieved through the whole mechanism. In next two sections we briefly recall two special cases, which occupy a prominent position in the present day applications of these modulation schemes.

5.2 - TCM

Trellis code modulation is a generalization of the combining principle first considered by Ungerboeck. This technique is reminiscent of the convolutional encoding, in fact in several important cases it is based on convolutional codes. It can be abstractly described as follows:

> Each signal of duration T, to be sent on the channel, is selected from a collection of point sets $\mathcal{X}_i$ where each set $\mathcal{X}_i$ is labeled by means of a block of k_s symbols that belongs to an alphabet of q symbols. In the same manner every point in $\mathcal{X}_i$ is labeled by means of of a block of k_t symbols from the same alphabet. The modulator is composed by a shift register having $k_s + k_t$ positions; every T seconds k_t symbols sequentially enter the register and a block of k_s symbols remains from the previous step to define the register state. Therefore a block of k_s symbols is used to select a subset $\mathcal{X}_i$ whereas a block of k_t symbols is used to select a point within the subset.
> Referring to the set $\mathbf{X} = \bigcup_i \mathcal{X}_i$ as a group code, it must have $q^{k_s+k_t}$ points and letting a two stage decomposition induced by q^{k_s} cosets, with q^{k_t} elements in each cosets. (Note that in the Ungerboeck original proposal we had $k_t = 1$ and $q = 2$).

5.3 - BCM

Block code modulation has been considered first by Imai and Hirakawa [42], and by Ginzburg [38], who introduced the following combination principle:

> Consider L codes $C_i = \{c_\ell\}_{\ell=1}^{M_i}$ of the same length N, respectively over alphabets of q_i symbols.
> Consider a set $\mathcal{S} = \{s_i(t)\}_{i=1}^{M}$ of $M = \prod_{i=1}^{L} q_i$ signals of duration T, therefore each block of $L \times N$ code symbols is associated to a signal of duration NT obtained by concatenating N elementary signals of duration T. Note that $\mathcal{S}$ possibly is a group code. At the j-th time interval the elementary signal $s_{u(j)}(t)$ is selected by means of a function of L variables
>
> $$u(j) = f(c_{j1}, c_{j2}, \ldots, c_{jL}) \quad .$$
>
> where the entries c_{ji} are the symbols that occupy the position j in the codeword $(c_{1i}, c_{2i}, \ldots, c_{Ni})$ of the code C_i.
> The transmitted signal, of duration NT, results
>
> $$S(t) = \sum_{j=1}^{N} s_{u(j)}(t - [j-1]T) \quad .$$
>
> The partition of the group code is used to define the function $f(.)$.

5.4 - Demodulation

The transmitted signal, corrupted by the noise during the propagation on the channel, will be received as

$$r(t) = S(t) + \nu(t) \quad .$$

At the receiver side the demodulation is a process intended to recover the signal $S(t)$ from $r(t)$ according to some appropriated decision rule.
Therefore assuming minimum distance detection, the problem will be to find the useful signal nearest to $r(t)$. Hence the N distances $\|r(t) - S(t)\| \quad S(t) \in \mathcal{P}$ should be computed and the demodulated signal will correspond to the minimum one. The number of necessary comparisons, for picking up the minimum is N, which usually is a huge number that practically excludes this direct strategy. For this fact, in general, it is necessary to look for

techniques requiring a smaller number of comparisons, possibly yielding a sub-optimal, but of feasible complexity, detection.
It is immediately seen that one sub-optimal strategy is a stage demodulation as suggested by the modulation process itself. However if we want greatest advantages, then we must hopefully take into account the actual group structure. Obviously in this case the resulting demodulation strategy will not be of general application because it will strongly depend on that particular group structure.

The above general combining conditions have been considered in [10] with reference to the special class of generalized group alphabets. The validity of these combining principles is demonstrated by several interesting examples showing the coding gain that can be achieved.

6 - Error correcting Codes

Error correcting codes have been extensively studied and a vast bibliography exists which is reported in many books, however the old treatise by MacWilliams and Sloane is still unsurpassed and its monumental bibliography is remained one of the most complete complete until 1977, [47]. After the limited use of error correcting codes at their beginnings, in the early sixties, now they play a determinant part in many areas:

1) deep space communications,

2) compact disc and

3) RF channels for mobile communications.

In most of these applications linear codes have been used because of their simple mathematical definition, simple encoder structures and well understood performance. Also several non-linear codes present many features that are reminiscent of the linear property and in many cases have a greater rate with the same minimum distance.
As initially said, decoding operations are intrinsically hard because their need of inverting a *non-invertible* function. Moreover the relations among different protocol levels contributes to make their position even more difficult.

6.1 - Encoding

A linear code over a finite field $\mathcal{F}$ is a k-dimensional subspace of a n-dimensional vector space $\mathcal{F}^n$. The characterization of such codes has a direct impact on the design of the encoder. Let us recall that through the generating matrix **G**, the n-dimensional code vector **c** is generated from a vector **x** of k-information bits according to the equation

$$\mathbf{c} = \mathbf{G}\mathbf{x} \quad .$$

This encoding algorithm can be advantageously applied to codes of short length or with few codewords.
Another approach is commonly followed for cyclic codes by describing the operations in terms of polynomial algebra. Assuming the polynomial representation for the codewords, i.e.

$$\mathbf{c} = (c_1, \ldots, c_n) \Leftrightarrow c(x) = \sum_{i=0}^{n-1} c_i x^i \quad ,$$

therefore a cyclic code is defined by a generating polynomial $g(x)$. The algorithm to be implemented for the systematic encoding of a cyclic code performs the following algebraic operations

$$c(x) = x^{n-k} I(x) + r(x)$$

where

- $r(x) = x^{n-k} I(x) \bmod g(x)$;
- $I(x)$ is the polynomial of information bits.

Several classes of non-linear codes admit encoding procedures that are not very different from the linear one and in particular circumstances may be preferable. Let us recall the definition of the class of non-linear codes with a good internal structure.

Definition 1 - *Let us consider a linear code with generating matrix* **G** *of dimension* $n \times k_1$ *and a matrix* **K** *of dimension* $n \times k_2$, *whose columns can be considered a subset of the coset leaders for the linear code generated by* **G**. *Therefore a non-linear code of length* n *and dimension* $k = k_1 + k_2$ *consists of the set of codewords*

$$\mathbf{c} = \mathbf{G}\mathbf{x}_1 + \mathbf{k}(\mathbf{x}_2) \quad .$$

where:

- *the information vector is decomposed as* $\mathbf{x} = (\mathbf{x}_1 \mid \mathbf{x}_2)$
- *the vector* $\mathbf{x}_2$ *indexes the columns of matrix* $\mathbf{K}$.

A particular subclass of non-linear codes has been considered in [33] where many analogies with linear codes have been evidenced and demonstrated.

6.2 - Decoding

Error-correcting codes may have different targets at the receiving front end, leading to different decoder structures, but more important yielding different protocols in order to manage the detected error situations.
In our approach we consider complete decoding only, because the effects of higher protocol levels are beyond our scopes restrained at the communication level.
To these aims the symbol error probability after decoding is the only significative code performance figure. Moreover it is by now an accepted fact that to get either the minimum word error probability or the bit error probability, normally different decoding strategies must be adopted. It is well known, see [3], that the Maximum Likelihood criterion minimizes the word error probability while a more complex criterion, which depends even on the code, is necessary to minimize the average bit error probability [5].
Let us now briefly recall some decoding criteria that will be applied in the design of the decoders. Let $\mathbf{r}$ denote the received vector.

ML criterion The Maximum Likelihood criterion selects the transmitted codeword $\hat{\mathbf{c}}$ that corresponds to the minimum conditional probability given $\mathbf{r}$.
For block codes over the binary symmetric channel the minimum distance decoding is maximum likely, and for the decoding operation it can be viewed as a standard array decoding with coset leaders of minimum Hamming weight.

UCL criterion The Unique Coset Leader criterion selects the coset leaders according to the following rule (binary codes):

- in cosets where the element of minimum weight is within the code error correcting capabilities, i.e. its weight is not greater than $\lfloor \frac{d-1}{2} \rfloor$, it is taken as coset leaders;
- otherwise take the unique element with all zeros in information positions.

Channel p(e)	(23,12,7)	(14,7,5)	(16,8,5)	(3,1,3)
5.5E-3	7E-4	9E-4	1.3E-3	9.E-5
1E-2	2.2E-3	1.14E-2	1.75E-2	3.E-4
5.9E-2	2.3E-1	3.1E-1	3.47E-1	1.E-2
9.9E-2	5.9E-1	6.58E-1	7.1E-1	2.7E-2

$aEb = a\ 10^b$

Table 1: Comparison of code performance over RF channels

An approach that considers communications links simply as carriers without looking at the use or meaning of the conveyed information practically must be bit oriented. As a consequence any performance measure must refer to the bit error probability of the overall chain. In this case the main purpose is to minimize the bit error probability after complete decoding. Therefore for many classes of good and practically interesting codes the **UCL** decoding strategy assumes a definitive position of prominence because it is almost always easier to implement and gives a smaller BER.

The comparison of error correcting codes with rate of the same order shows that there is a conservative law in their performance that allows to foresee code behaviors and their order. In table 1 some comparison of measured error probability of codes working on RF channels are reported for sake of comparison. Here beside the theoretical limit computed for the repetition code $(3,3,3)$, the residual error probability for Golay $(23,12,7)$ code, the Preparata $(14,7,5)$ code and Kerdock $(16,8,5)$ code are considered.

6.3 - RS encoding

As an example of application of the algorithms that extensively use finite field arithmetic in particular multiplications, let us consider the co/decoding of Reed-Solomon codes, which are cyclic codes (satisfying the Singleton bound). The product of polynomials is used to encode information symbols with operations performed in $GF(2^m)$. The RS code (n,k,d) with $n \geq d \geq 3$, $k = n - d + 1$ and generating polynomial $g(x) = \prod(x - \alpha^i)$ is considered. This code may correct ν errors and γ erasures provided that the

constraint

$$2\nu + \gamma \leq d-1 \quad 0 \leq \nu \leq \frac{d-1}{2} \quad and \quad 0 \leq \gamma \leq d-1$$

is satisfied. For all subsequent discussions we assume that the code is systematic, therefore the encoder implements algorithms that perform a division of $I(x)\ x^{d-1}$ by $g(x)$ to produce the remainder $r(x)$ that allows us to write the codeword in the form:

$$c(x) = I(x)\ x^{d-1} + r(x) \quad .$$

For the description of structures that perform efficiently see [11], while as regard to the finite field arithmetic that are needed we refer to section 7 of this report.

6.4 - RS decoding

In this section we briefly review a decoding algorithm that considers either erasure and error correction for RS codes because the combined algorithm seems to have not received a great attention. In fact, the error correction has been thoroughly studied and the Berlekamp-Massey algorithm represents the first efficient solution to the problem of the error allocation while Forney's error evaluation is an efficient solution in case of non binary codes. Starting from the clever formulation of the error correction for cyclic codes due to Peterson, Gorenstein and Zierler through Berlekamp's ideas a lot of algorithms with different implementation have been proposed, for this reason we do not discuss any-more the problem of error correction but we consider only the situation with erasure at the RS decoder input.

Complete decoding of RS codes with the minimum distance criterion is practically impossible because the covering radius of these codes are always $d-1$ which means that we have cosets leaders of any weight. Moreover for codes of reasonable dimension the distribution of the weight of the coset leader is not even known.

Therefore the UCL decoding is unavoidable but the problem of the correction of erasures still remains. However resorting to the classical approaches due to Peterson, Gorenstein and Zierler it is immediately seen that erasure correction and error correction can be performed independently, in particular we may correct first the erasures and then apply the Berlekamp-Massey algorithm to find the errors location and then apply Forney's algorithm to find error magnitudes.

The procedure is based on the computation of syndromes and consists of the following formal steps:

step 1. compute $d-1$ syndromes;

step 2. correct the erasures

step 3. re-compute the $d-1$ syndromes;

step 4. correct the errors;

step 5. if the condition $2\nu+\gamma \leq d-1$ is not accomplished then to decode the information symbols with no action, the erasures in this case are substituted with symbols randomly generated.

6.4.1 - Decoding algorithm

Now we describe in detail the first two steps of the above plan, because they seem to be overlooked by the specialized literature. Next steps instead have received such a wide attention that we simply refer to the dedicated books, for example to the excellent [11, 51].

As said before the approach is classically due to Peterson, Gorenstein and Zierler and consists in writing down a set of $d-1$ equations in $2\nu+\gamma$ unknowns (error magnitude and positions and erasure magnitudes) as a consequence of the syndromes

$$S_1 = r(\alpha), \quad S_2 = r(\alpha^2), \quad \ldots \quad , \quad S_{d-1} = r(\alpha^{d-1}) \quad ,$$

where erasures have been substituted with the 0 symbols for simplicity, any other symbol works as well. The system results

$$\begin{cases} S_1 &= Y_1X_1 + Y_2X_2 + \ldots + Y_\nu X_\nu + Y_{\nu+1}Z_{\nu+1} + \ldots + Y_{\nu+\gamma}Z_{\nu+\gamma} \\ S_2 &= Y_1X_1^2 + Y_2X_2^2 + \ldots + Y_\nu X_\nu^2 + Y_{\nu+1}Z_{\nu+1}^2 + \ldots + Y_{\nu+\gamma}Z_{\nu+\gamma}^2 \\ & \vdots \\ S_{d-1} &= Y_1X_1^{d-1} + Y_2X_2^{d-1} + \ldots + Y_\nu X_\nu^{d-1} + Y_{\nu+1}Z_{\nu+1}^{d-1} + \ldots + Y_{\nu+\gamma}Z_{\nu+\gamma}^{d-1} \end{cases}$$

where

- Yi denote either error or erasure magnitude;

- $X_i = \alpha^{\ell_i}$ denote the error position;

- $Z_i = \alpha^{f_i}$ denote the known erasure position.

Let us introduce the syndrome generating polynomial

$$S(z) = \sum_{i=0}^{d-2} S_{i+1} z^i \quad ,$$

so that the above system can be written as a polynomial too

$$S(z) = \sum_{i=1}^{\nu} Y_i X_i \frac{1 - (X_i z)^{d-1}}{1 - X_i z} + \sum_{i=1}^{\gamma} Y_{i+\nu} Z_i \frac{1 - (Z_i z)^{d-1}}{1 - Z_i z} \quad .$$

Considering $S(z)$ modulo z^{d-1}, we get the simplification

$$S(z) = \sum_{i=1}^{\nu} Y_i X_i \frac{1}{1 - X_i z} + \sum_{i=1}^{\gamma} Y_{i+\nu} Z_i \frac{1}{1 - Z_i z} \quad .$$

Introduced the polynomial

$$R(z) = \prod_{i=1}^{\nu} (1 - X_i z) \quad .$$

hence multiplying $R(z)$ by $S(z)$ and taking the result modulo z^{d-1} we get Forney's polynomial for erasure magnitude estimation

$$\Omega(z) = S(z) R(z) \pmod{z^{d-1}} \quad .$$

Evaluating $\Omega(z)$ in the roots X_i^{-1} of $R(z)$ we have

$$\Omega(X_i^{-1}) = -Y_i X_i R'(X_i^{-1}) \quad ,$$

and in conclusion

$$Y_i = -\frac{\Omega(X_i^{-1})}{X_i R'(X_i^{-1})} \quad ,$$

where $R'(z)$ denotes the formal derivative of $R(z)$.

At this point syndromes are updated, thus the Berlekamp-Massey algorithm and again the Forney method are used to evaluate the error magnitude.

The correcting algorithms are mathematically described, so for implementation purposes, it is assumed that any arithmetical operation in the proper finite field is realized by some specialized device:

1. addition
2. product
3. powers
4. fractional powers, i.e. square, cube roots etc.

The circuits that perform these operations are built following some generally accepted design principles that lead to efficient circuitry, that is 1) modularity, 2) algorithms with small overhead and 3) possibility of large scale integration (VLSI).

6.5 - Code concatenation

Code concatenation is a flexible scheme that allows to achieve good compromises among available resources. The importance of flexible, efficient and economic co-decoding schemes needs not to be explained as the use of codes is becoming more and more important in the design of transmission systems either for satellite links, broadcast distribution or fiber optical transmission.

It concerns the concatenation of binary linear codes both block and convolutional and shows that concatenation is not a commutative operation. The asymptotic expression of the resulting bit error probability for several interesting pairs of concatenated block codes are also derived discussed with respect to decoding complexity and decoding delays.

In the paper [31] these aspects of the concatenation are considered, in particular the problem of threshold, below which codes are useless, are analyzed as well as the exact error probability evaluation at high channel bit error probability, conditions that frequently happen when the operating conditions are severe and error rate of 10^{-2} are common figure.

7 - Complexity considerations

Error correcting codes with high correcting capabilities require high speed computations in proper fields in order to perform their tasks in a transparent way to the users. Operations in finite fields are more reliable than in real fields because of the lack of rounding. However to get high throughput they must be executed at high speed, a not easy task if the order of the field is large.

In [41] a comparison of VLSI architectures of Finite Field multipliers using different basis representations is clearly presented. Three widely used multiplication algorithms are analyzed

- dual basis multiplier due to Berlekamp
- normal basis multiplier due to Massey-Omura
- standard basis multiplier due to Scott-Tavares-Peppard

and advantages and disadvantages are clearly illustrated. We think that one more multiplier scheme that takes into account the structure of irreducible polynomials associated to base generating elements (standard basis) should be conveniently considered. This is the basic idea described in [35]. The algorithm is suitable either for software implementation or VLSI implementation. It seems very efficient and easy to deal with, the only reservation concerns the fact that we know only a finite number of such polynomials and it is unproved whether an infinite number exist or not. However for many practically interesting cases we have such polynomials.

The structure of any multiplier is recalled in fig. 2, where the difference among the several algorithms is in the implementation of the XOR-ing block. Of course algorithms that require dual basis need a pre-conversion of the input bits.

In [41] referring to the arithmetics in $GF(2^8)$ suitable for dealing with standard RS (255, 223) codes, with respect to the dual basis multiplier the irreducible polynomial of degree 8 is chosen to be

$$x^8 + x^4 + x^3 + x^2 + x + 1 \quad .$$

However in this field is available an irreducible primitive polynomial of the form

$$x^8 + x + 1$$

that allows us to use the most advantageous algorithm proposed in [35].

As decoding algorithms for RS codes need also efficient evaluations of powers a short discussion about this problem is in order. This discussion is even more important because in finite field the inverse computation, or division, is equivalent to power evaluation. In fact, in $GF(q)$, we have

$$\alpha^{-1} = \alpha^{q-2} \quad .$$

The question connected with the minimum number of multiplications necessary to compute a power is considered in particular. Two situations are common:

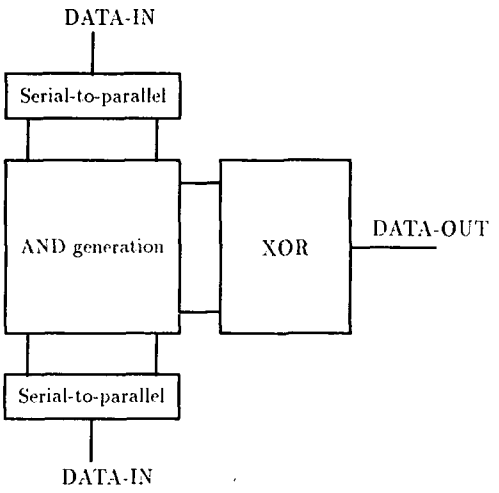

Figure 2: The block diagram of a multiplier for finite field elements

- To compute powers β^n with the exponent n known and fixed, therefore the optimal power computation rule can be defined one time and forever;
- To compute powers β^n with the exponent n unknown, suboptimal rules should be used, because to find the optimal one is usually computationally hard.

In [32] we have analyzed the situation and reported some comments on a long-standing conjecture on the computation of powers.

8 - Conclusions

In this report we have briefly reviewed some points that are basic in the design of signal sets for communications channels working under burdensome

conditions. In particular we have evidenced several relevant components

- base signals
- point configurations
- combination of coding and modulation
- arithmetical operations in finite fields.

We have seen that signal processing is the tool for pursuing the objectives promised by the Shannon theory. In other terms digital signal processing allows us to exchange computational complexity for bandwidth or energy. Shannon's approach should have hopefully gained insight on the system performance by dealing independently with single blocks, functionally well defined. The underlying idea was that local optimization would be easier and should have lead to an optimal performance of the whole system. On the contrary Ungerboeck has shown that global optimization can produce better effects than the step by step optimization strategy implicitly suggested by the Shannon channel model.

9 - List of Research Papers

1. **E.Biglieri, M.Elia,** Multidimensional Modulation and Coding for Bandlimited Digital Channels, *IEEE Transactions on Information Theory*, vol.IT-34, n.4, July 1988, pp.803-809.

2. **E.Biglieri, S.Barberis, M.Catena,** Analysis and Compensation of Nonlinearities in Digital Transmission Systems, *IEEE Journal on Selected Areas in Communications*, January 1988.

3. **M.Elia,** Group Codes and Signal Design for data Transmission, *ISICT'87*, Campinas, Brasile, July 1987.

4. **M.Elia, F.Neri,** A Note on Addition Chains and Some Related Conjectures, *Advanced Inter. Workshop on SEQUENCES. Combinatorics, Compression. Security and Transmission*, Salerno, Italy, June 1988, pp.166-181.

5. **M.Elia, C.Losana, F.Neri,** A Note on the Complete Decoding of Kerdock Codes, *IEEE International Symposium on Information Theory*, Kobe, Japan, June 1988.

6. **M.Elia, D.Vellata,** Multiplication in Galois Field $GF(2^m)$, *Internal Report*, June 1988.

7. **M.Elia, F.Neri,** On the Concatenation of Binary Linear Codes, submitted to *IEEE Transactions on Communications*, 1989.

References

[1] **J.Adoul,** Fast ML Decoding Algorithm for the Nordstrom-Robinson Code, *IEEE Transactions on Information Theory* vol. IT-33, N. 6, Nov. 1987, pp. 931-933.

[2] **M.Ajmone-Marsan et al.,** Digital Simulation of Communication Systems with TOPSIM, *IEEE Journal Select. Areas in Communications*, vol. SAC-2, n. 1, Jan. 1984, pp. 42-50.

[3] **E.R.Berlekamp,** *Algebraic Coding Theory*, McGraw-Hill Book Company, New York, 1968.

[4] **E.R.Berlekamp,** Bit-serial Reed-Solomon encoders, *IEEE Transactions on Information Theory*, vol.IT-28, November 1982, pp.869-874.

[5] **E.R.Berlekamp, H.Rumsey, G.Solomon,** On the Solution of Algebraic Equations over Finite Fields, *Information and Control*, 10, October 1978, pp. 553-564.

[6] **E.Biglieri,** High-level modulation and coding for nonlinear satellite channels, *IEEE Transactions on Communications*, vol.COM-32, May 1984, pp.616-626.

[7] **E.Biglieri, M.Elia.** Cyclic-group codes for the gaussian channel, *IEEE Transactions on Information Theory*, vol.IT-22, n.5, September 1976, pp.624-629.

[8] **E.Biglieri, M.Elia.** Optimum Permutation Modulation Codes and Their Asymptotic Performance, *IEEE Transactions on Information Theory*, vol.IT-22, n.6, November 1976, pp.751-753.

[9] **E.Biglieri, M.Elia.** On the existence of group codes for the Gaussian channel, *IEEE Transactions on Information Theory*, vol.IT-18, May 1972, pp.399-402.

[10] **E.Biglieri, M.Elia,** Multidimensional Modulation and Coding for Bandlimited Digital Channels, *IEEE Transactions on Information Theory*, vol.IT-34, n.4, July 1988, pp.803-809.

[11] **R.Blahut.** *Theory and Practice of Error Control Codes*, Addison-Wesley, New York, 1983.

[12] **I.F.Blake, R.C.Mullin**, *The Mathematical Theory of Coding*, Academic Press, New York, 1975.

[13] **A.Borodin, I.Munro**, *The Computational Complexity of Algebraic and Numeric Problems*, American Elsevier Pub., New York, 1975.

[14] **P.Bours, J.C.M.Janssen, M.vanAsperdt, H.C.A.vanTilborg**, Algebraic Decoding beyond e_{BCH} of some binary cyclic codes, when $e > e_{BCH}$, *International Colloquium on Coding Theory*, Osaka, 1988.

[15] **A.R.Calderbank, J.E.Mazo, H.M.Shapiro**, Upper bounds on the minimum distance of trellis codes, *Bell Syst. Tech. Journal*, vol. 62, October 1983, pp.2617-2646.

[16] **A.R.Calderbank, N.J.A.Sloane**, Four-Dimensional Modulation with an Eight-State Trellis Code, *AT&T Tech. Journal*, Vol.64, No.5, May-June 1985, pp.1005-1018.

[17] **R.Calderbank, J.E.Mazo**, A new description of trellis codes, *IEEE Transactions on Information Theory*, vol.IT-30, November 1984, pp.784-791.

[18] **C.L.Chen**, Formulas for the Solutions of Quadratic Equations over $GF(2^m)$, *IEEE Transactions on Information Theory*, vol. IT-28, no. 5, September 1982, pp. 792-794

[19] **G.C.Clark, J.B.Cain**, *Error-Correction Coding for Digital Communications*, Plenum Press, New York, 1981.

[20] **J.H.Conway, N.J.A.Sloane**, Soft decoding techniques for codes and lattices, including the Golay code and the Leech lattice, *IEEE Transactions on Information Theory*, vol. IT-32, Jan. 1986, pp. 41-50.

[21] **D.Divsalar, J.H.Yuen**, Asymmetric MPSK for trellis codes, *GLOBECOM '84*, Atlanta, GA, November 26-29, 1984, pp.20.6.1-20.6.8.

[22] **D.Divsalar, M.K.Simon**, Combined trellis coding with asymmetric modulations, *GLOBECOM '86*, New Orleans, Louisiana, Dec.2-5, 1985, pp.21.2.1-21.2.7.

[23] **L.A.Dunning**, Encoding and Decoding for the Minimization of Message Symbol Error Rates in Linear Block Codes, *IEEE Transactions on Information Theory*, vol.IT-33, n.1, January 1987, pp.91-104.

[24] **G. Einarsson et al.,** *Topics in Coding Theory* Lecture Notes in Control and Information Sciences, Springer Verlag, Berlin, 1989.

[25] **M.Elia,** Algebraic decoding of the (23,12,7) Golay Code, *IEEE Transactions on Information Theory*, vol.IT-33, January 1987, pp.150-151.

[26] **M.Elia,** A note on the computation of bit error rate for binary block codes, *Journal of Linear Algebra and its Applic.*, vol.98, January 1988, pp.199-210.

[27] **M.Elia**, Symbol error rate of binary block codes, *Trans. Ninth Prague Conference on Inform. Th., Statist. Dec. Functions, Random Processes*, Prague, pp.223-227, June 1982.

[28] **M.Elia,** Group Codes and Signal Design for data Transmission, *ISICT'87*, Campinas, Brasile, July 1987.

[29] **M.Elia, M.T.Galizia Angeli,** Autofunzioni di operatori lineari integrali associati ai filtri di Butterworth, *GMEL*, Coimbra, 1985, pp.61-64.

[30] **M.Elia, M.T.Galizia Angeli,** Eigenfunctions of Integral Linear Operators Associated to Second Order Filters, Proceedings of the International Symposium Modelling, Identification and Control, *IASTED*, Grindelwald, 1987, pp.396-399.

[31] **M.Elia, F.Neri,** On the Concatenation of Binary Linear Codes, *Internal report*, 1989.

[32] **M.Elia, F.Neri,** A Note on Addition Chains and Some Related Conjectures, *Advanced Inter. Workshop on SEQUENCES, Combinatorics, Compression, Security and Transmission*, Salerno, Italy, June 1988, pp.166-181.

[33] **M.Elia, C.Losana, F.Neri,** A Note on the Complete Decoding of Kerdock Codes, *IEEE International Symposium on Information Theory*, Kobe, Japan, June 1988.

[34] **M.Elia, G.Prati.** On the Complete Decoding of Binary Linear Codes, *IEEE Transactions on Information Theory*, vol.IT-31, no.4, July 1985, pp.518-520.

[35] **M.Elia, D.Vellata,** Multiplication in Galois Field $GF(2^m)$, *Internal Report*, June 1988.

[36] **M.Franck**, *Signal Theory*, Prentice Hall, 1970

[37] **A.Gersho, V.Lawrence**, Multidimensional signal design for digital transmission over bandlimited channels, *Proceedings of ICC'84*, Amsterdam, The Netherlands, May 1984, pp.377-380.

[38] **V.V.Ginzburg**, Mnogomerniye signaly dlya nepreryvnogo kanala, *Problemy Peredaci Informacii*, n.1, 1984, pp.28-46, (in Russian).

[39] **J.Hartmanis,** Feasible computations and Provable complexity Properties, *SIAM, CBMS-NSF series*, Philadelphia, 1978.

[40] **C.R.P.Hartmann, K.K.Tzeng,** Decoding beyond the BCH bound using multiple sets of Syndrome Sequences, *IEEE Transactions on Information Theory*, vol. IT-20, 1974, pp. 292-295.

[41] **I.S.Hsu, T.K.Troung, L.J.Deutsch, I.S.Reed,** A Comparison of VLSI Architecture of Finite Field Multipliers Using Dual, Normal or Standard Bases, *IEEE Transactions on Computers*, vol.C-37, No.6, June 1988, pp.735-739.

[42] **H.Imai, S.Hirakawa**, A new multilevel coding method using error-correcting codes, *IEEE Transactions on Information Theory*, vol.IT-23, 1977, pp.371-377.

[43] **I.Jacobs**, Comparison of M-ary modulation systems, *Bell System Technical Journal*, vol.46, May-June 1967, pp.843-864

[44] **A.M.Kerdock,** A class of low-rate nonlinear codes, *Information and Control*, 20 (1972), pp. 182-187.

[45] **D.E.Knuth,** *The Art of Computer Programming*, vol. II, Addison-Wesley, Reading Massachussetts, 1981.

[46] **F.J.MacWilliams**, A Theorem on the distribution of weights in a Systematic Code, *BSTJ*, 42, 1962, pp.79-94.

[47] **F.J.MacWilliams, N.A.J.Sloane,** *The Theory of Error Correcting Codes*, North Holland, Amsterdam, 1977.

[48] **R.J.McEliece,** *The Theory of Information and Coding*, Addison-Wesley, Reading Mass., 1977.

[49] **R.J.McEliece,** *Finite Fields for Computer Scientists and Engineers,* Kluwer Academic Press, Boston, 1987.

[50] **A.Papoulis,** *Signal Analysis,* McGraw Hill, New York, 1977.

[51] **W.W.Peterson, E.J.Weldon,** *Error-Correcting Codes,* MIT Press, Cambridge, 1981.

[52] **P.G.Petrovsky,** *Lectures on the theory of integral equations,* MIR, Mosca, 1971.

[53] **P.A.Scott, S.E.Tavares, L.E.Peppard,** A fast multiplier for $GF(2^m)$, *IEEE Journal on Selected Areas in Communications,* vol.SAC-4, January 1986.

[54] **Shu Lin, D.J.Costello.** *Error Control Coding: Fundamentals and Applications,* Prentice-Hall, Englewood Cliffs, New Jersey, 1983.

[55] **D.Slepian.** Some Comments on Fourier Analysis, Uncertainty and Modeling, SIAM Review, Vol.25, No.3, pp.379-393, July 1982.

[56] **D.Slepian.** Bounds on Communication, *Bell System Technical Journal,* vol.42, May 1963, pp.681-707.

[57] **D.Slepian.** A Class of Binary Signaling Alphabets. *BSTJ.* v.35, pp.203-234, January 1956.

[58] **D.Slepian.** Group codes for the Gaussian channel. *Bell System Technical Journal,* vol.47, April 1968, pp.575-602.

[59] **N.J.A.Sloane.** *A Short Course on Error-correcting Codes.* CISM course N.188, Springer, Wien, 1975.

[60] **G.Ungerboeck.** Channel coding with multilevel/phase signals, *IEEE Transactions on Information Theory,* vol.IT-28, January 1982, pp.55-67.

[61] **A.W.M.vanDen Enden, N.A.M.Verhoeckx.** *Discrete-Time Signal Processing. An Introduction,* Prentice-Hall, Englewood Cliffs, New Jersey, 1989.

[62] **J.H.vanLint.** *Introduction to Coding Theory,* Springer Verlag, New York, 1982.